~~SECRET~~

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

(U) Office of Inspector General Laptop Computers Are Susceptible To Compromise (Unclassified and Redacted)

The Department of Homeland Security, Office of Inspector General, has redacted this report for public release.

Office of Information Technology

OIG-06-58 **August 2006**

~~SECRET~~

(Classification is UNCLASSIFIED when separated from Appendices B & D)

~~SECRET~~

(Classification is UNCLASSIFIED when separated from Appendices B & D)

Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 8, 2006

Preface

(U) The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

(U) This report assesses the strengths and weaknesses of OIG laptop computer security controls. It is based on interviews with OIG officials, direct observations, technical tests, and a review of applicable documents.

(U) The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank W. Deffer
Assistant Inspector General for Information Technology

~~SECRET~~

(U) Table of Contents/Abbreviations

(U) Appendices

(U) Abbreviations

(U) ATL Advanced Technology Laboratory
(U) [redacted]
(U) C&A Certification and Accreditation
(U) CIO Chief Information Officer
(U) CSIRC Computer Security Incident Response Center
(U) [redacted]

(U) Table of Contents/Abbreviations

(U) DHS	Department of Homeland Security
(U) FIPS	Federal Information Processing Standards
(U) FISMA	Federal Information Security Management Act of 2002
(U) IP	Internet Protocol
(U) ISSM	Information Systems Security Manager
(U) IT	Information Technology
(U) NIST	National Institute of Standards and Technology
(U) NSA	National Security Agency
(U) [redacted]	[redacted]
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) PED	Portable Electronic Device
(U) POA&M	Plan of Action and Milestones
(U) SBU	Sensitive But Unclassified
(U) SP	Special Publication
(U) ST&E	Security Test and Evaluation

(U) Executive Summary

(U) We audited the Department of Homeland Security (DHS) and its organizational components' security program to evaluate the security and integrity of select government-issued laptop computers. The OIG has employed many essential security controls for its SBU and classified laptops. Specifically, the OIG has developed a standard configuration for its SBU laptops, as well as procedures to patch and update SBU laptop computers that are routinely connected to the OIG Network. Further, the OIG has established adequate physical security measures for its laptops and has implemented many of the security program requirements for its classified system that contains the OIG's laptops and desktops. The OIG Network includes SBU laptops and desktops.

(U) Significant work remains for the OIG to further strengthen the configuration, patch, and inventory management controls necessary to protect its government-issued laptop computers. Specifically, the OIG has not: (1) implemented a standard configuration, that meets required minimum-security settings for both its SBU and classified laptops; (2) established effective procedures to patch laptop computers that are not regularly connected to the OIG Network; (3) maintained an accurate inventory; (4) cleared sensitive data from laptops prior to reuse within the organization; and, (5) applied the appropriate classification labels or markings. In addition, a number of concerns were noted on the OIG's classified laptops. The results of OIG classified laptops are summarized in Appendix D.

(U) We recommend that the Assistant Inspector General for Administrative Services instruct the Chief Information Officer (CIO) to:

- (U) Remedy the existing critical vulnerabilities in the standard configuration for SBU laptops, and determine whether similar vulnerabilities and remediation are relevant to all government-issued computers.
- (U) Establish procedures to ensure that model systems are configured to protect OIG data and verified prior to implementation.

- (U) Develop procedures to ensure that all OIG laptops are patched and updated in a timely manner.
- (U) Implement an enterprise property management system to ensure an accurate laptop inventory is maintained, and that all laptop computers are handled in accordance with OIG inventory management policies and procedures.
- (U) Clear or sanitize laptop computers before reissue or disposal, and ensure that classified and SBU laptops are labeled appropriately.
- (U) Develop a risk assessment for the OIG Network, test the contingency plan, and provide specialized privacy training to relevant officials.

(U) Recommendations related to classified laptops are included in Appendix D. See Appendix A for our purpose, scope, and methodology.

(U) In response to our draft report, the Assistant Inspector General for Administration concurred with our recommendations and is in the process of implementing corrective measures. In addition, plan of action and milestones will be created and tracked for the vulnerabilities we identified. The OIG's unclassified response is summarized and evaluated in the body of this report and its classified response is summarized and evaluated in Appendix D. The OIG's entire response is included as Appendix B.

(U) Background

(U) As the weight and price of laptops have decreased and their computing power and ease of use have increased, so has their popularity for use by government employees. DHS is heavily reliant on laptop computers for conducting business.[1] The mobility of laptops has increased the productivity of the workforce, but at the same time increased the risk of theft, unauthorized data disclosure, and virus infection. Thefts of laptop computers occur regularly from offices, airports, automobiles, and hotel rooms, and the incidence of laptop thefts is increasing. In 2005, 12 security incidents involving stolen DHS laptops were reported to the DHS Computer Security Incident Response Center (CSIRC), including government-issued laptops from U.S. Customs and Border Patrol, United States Secret Service, U.S. Immigration and Customs Enforcement, and the Science and Technology Directorate.

(U) Government organizations that provide for the use of laptop computers must take steps to ensure that the equipment and the information that is stored on them are adequately protected. Such steps may include ensuring secure storage of laptop computers when they are not in use, encrypting data files stored on laptops, installing adequate security software applications such as firewalls and anti-virus software, disabling and controlling built-in wireless, Bluetooth, and infrared connection capabilities, and regularly updating operating system and application software.

(U) *DHS Sensitive Systems Policy Publication 4300A* and *DHS National Security Systems Policy Publication 4300B* provide direction to DHS components[2] regarding the management and protection of sensitive and classified systems.[3] These policies outline the management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity within the DHS information technology (IT) infrastructure and operations. DHS policy requires that its components ensure that strong

(U) [1] Our technical tests included 94 sensitive but unclassified (SBU) laptops, and 8 classified laptop computers.
(U) [2] DHS "organizational components" are defined as directorates and major component agencies.
(U) [3] In this report, we refer to *DHS Sensitive Systems Policy Publication 4300A* and *DHS National Security Systems Policy Publication 4300B* collectively as "DHS policy."

inventory management, physical security, logical access, and wireless security controls are implemented for all systems processing sensitive or classified information. The department developed the DHS Sensitive Systems Handbook and National Security Systems Handbook to provide specific techniques and procedures for implementing the requirements of DHS policy. Further, in August 2005, DHS issued a series of secure baseline configuration guides for certain operating system and software applications, such as Microsoft Windows XP.

(U) NIST has issued several publications related to laptop inventory management, physical security, logical access, and wireless security controls. Specifically, NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance for establishing adequate logical and physical access controls for sensitive government systems, including the use of strong passwords, encryption, and user administration practices. Further, [redacted][4]

(U) The *Federal Information Security Management Act of 2002* requires each agency to develop, document, and implement an agency-wide information security program to provide security for its information and systems. Policies should ensure that information security is addressed throughout the life cycle of each agency information system and determine minimally acceptable system configuration requirements.

(U) [4] [redacted]

(U) Results of Audit

(U) Standard Configurations Will Enhance Laptop Security

(U) The OIG does not have a secure standard configuration for its laptop computers. We evaluated the process used by the OIG to develop a standard configuration for its laptop and desktop computers. Also, we conducted computerized and manual security tests of the model system to ensure that it was configured in conformance with DHS and federal guidelines. Finally, we tested a sample of 94 primary, secondary, and loaner laptop computers to determine whether the OIG had effectively applied its model system.[5] These tests included:

- (U) Automated vulnerability assessment testing and port scanning of all 94 laptops to identify configuration weaknesses.
- (U) Detailed technical testing for a subset of 25 laptops to confirm the automated testing results and determine account, audit, access privilege, and password parameter settings.
- (U) Manual reviews for a subset of 31 laptops to verify the presence and configuration of installed software.

(U) The laptop model system fails to establish the required minimum-security for laptop computers as directed by DHS. In addition, the OIG has not ensured that the model system is consistently implemented on all OIG laptops. For example, [redacted] Finally, because the OIG used the same process to develop the standard configuration for both its laptop and desktop computers, the configuration weaknesses are relevant to all OIG government-issued computers. As a result of the security issues identified, sensitive data may not be adequately protected.

(U) [5] To adequately perform vulnerability assessment tests and not penetration tests, the audit team was provided administrator access to the OIG model system and laptops, and disabled any personal firewalls on the laptops.

(U) SBU Model System Fails To Establish Minimum Security Settings

(U) The OIG has developed and implemented a model system for its SBU laptop computers. A model system, also referred to as a standard build or golden image, is a package of installed software with standardized configuration settings that is created for each major group of IT resources (e.g., routers, user workstations, file servers). The OIG model system was developed based on National Security Agency (NSA) workstation and DHS server configuration guidelines for Microsoft Windows 2000.[6] The OIG model system incorporates antivirus software, as well as a personal firewall for users that remotely access the OIG Network. The model system also includes the disabling of any built-in wireless capabilities. However, the OIG model system does not incorporate certain critical controls. Specifically, the model system does not:

- (U)
- (U)
- (U)
- (U)
- (U)

(U) [6] DHS has not issued configuration guidelines for workstations running Windows 2000 operating system. As a result, the OIG relied upon, to the extent possible, the DHS configuration guidelines for Windows 2000 Server.

[redacted][7]

- (U) [redacted][8]

(U) The OIG had not implemented [redacted] The other weaknesses are the result of the OIG not sufficiently testing the model system prior to implementation. For example, the [redacted] Based on the weaknesses identified, the OIG amended its laptop model system and requested that we test the new model. We verified that several of the weaknesses had been addressed, including [redacted] Further, the CIO stated that the OIG plans to formally accept the risk associated with the remaining vulnerabilities on the model system.

(U) DHS and NIST require that a model system be developed and implemented to ensure that a secure, standard configuration is implemented on desktop and laptop computers. According to NIST, standardized configurations reduce the labor involved in identifying, testing, and applying patches; and, encourage a higher level of consistency, which generally leads to improved security. Further, DHS requires that each fully supported operating system have a model system from which every computer is built.

(U) [7] [redacted]

(U) [redacted]

(U) DHS and NIST recommend that the [redacted] DHS and NIST also require that [redacted][9]

(U) As a result of the critical vulnerabilities and configuration weaknesses in the model system, OIG laptops and data are not protected adequately. For example, [redacted]

(U) Table 1 illustrates the number of high and medium risk configuration vulnerabilities on the OIG laptop model system, along with the corrective actions that the OIG has already taken or planned to address these weaknesses.[10]

(U) [9] [redacted]

(U) [10] [redacted]

(U)

	Number of Vulnerabilities Identified			Number of Vulnerabilities Addressed		
(U)						

(U) Source: OIG table based on the results of technical testing and interviews with OIG personnel.

(U) SBU Model System Has Not Been Implemented Uniformly

(U) The OIG has not implemented consistently its model system for SBU laptop computers. A model system is a read-only mechanism that is used to build new instances of the system. Once developed, the OIG model system is loaded onto a server as an "image" or copy. The image is then installed on new laptops prior to the computers being placed into operation of the 94 SBU laptops tested, 38 (40 percent) had configuration vulnerabilities not found on the model system. Most of these laptops had only one or two additional vulnerabilities. However, three of the tested laptops had a combined total of 28 additional configuration vulnerabilities, and thus deviated significantly from the model system.

(U) Table 2 illustrates the number of additional high and medium risk configuration vulnerabilities on OIG laptops listed by site and by type of laptop.

(U)

		Number Matching Model System					Total With 1 or More Weaknesses
Total	94	56 (60%)	18 (19%)	17 (18%)	2 (2%)	1 (1%)	38 (40%)
Headquarters							
Atlanta Office							
Denton Office							
Primary							
Secondary[(a)]							
Loaner							

(U) Source: OIG table based on the results of technical testing and interviews with OIG personnel.

(U) In addition, for the 31 SBU laptops included in our manual reviews, there was [redacted] For the 30 laptops with [redacted] in accordance with the model system.

(U) Further, of the 25 SBU laptops included in our detailed testing:

- (U) [redacted]
- (U) [redacted]

- (U) [redacted]
- (U) [redacted]

(U) According to the OIG Information Systems Security Manager (ISSM), the laptops included in our automated vulnerability scans, manual reviews, and detailed technical testing that deviated significantly from the model system were largely the result of the OIG not ensuring that all laptops go through its standard configuration and issuance process. For example, three laptops with a large number of additional configuration weaknesses were older laptops that came over to the OIG from the Department of Treasury when the DHS OIG was established. These laptops were supposed to be excessed, but instead remained in use. Another laptop was not configured appropriately because it was an evaluation unit. This unit was supposed to be turned in following the evaluation, but instead also remained in use.

(U) DHS policy requires that components establish, implement, and enforce change management and configuration management controls on all IT systems and networks. The DHS IT Security Architecture Guidance also advises that each fully supported operating system have a standard configuration from which every instance is built. According to NIST, standardized configurations reduce the labor involved in identifying, testing, and applying patches; and, encourage a higher level of consistency, which generally leads to improved security. DHS and federal configuration guidelines also establish requirements related to security parameter settings, including [redacted] As a result of the OIG not ensuring that all laptop computers are configured appropriately, users were [redacted]

[11]

(U) [11] [redacted]

(U) Improved Patch Management Will Increase Security

(U) The OIG has not established effective procedures to patch and update its laptop computers. We reviewed the OIG laptop model system to determine if all of the applicable operating system and application patches had been applied. In addition, we tested a sample of 94 SBU primary, secondary, and loaner laptop computers to determine if all appropriate patches had been applied. The OIG has procedures to patch laptops prior to being placed into operation by including patches and updates as part of the model system installation process. For laptops already in operation, the OIG patches and updates these laptops through the OIG Network by placing the updates on a server and then distributing them to connected laptop and desktop computers. However, there were patches and updates related to high and medium risk vulnerabilities that had not been applied. Specifically,

- (U) The OIG has not applied all relevant patches to laptops that regularly connect to the network. [redacted][12] The update had not been applied because the OIG does not have procedures to identify all relevant updates and patches. In addition, [redacted][13] [redacted][14] According to the ISSM, the two

(U) [12] [redacted]

(U) [13] [redacted]

(U) [14] A total of 62 user assigned laptops were tested. However, information regarding installed patches was not obtained for three laptops due to a software conflict.

patches had been uploaded for distribution to workstations on the OIG Network, but had failed to install. The OIG was not aware that the patches had failed to install prior to our review.

- (U) The OIG has not patched laptops that do not regularly connect to the network. For example, two loaner and two secondary unit laptops were missing a total of 160 additional high and medium risk patches. Further, for the [redacted] According to the ISSM, the loaner and secondary unit laptops were placed into operation before procedures were developed.

(U) Table 3 illustrates the number of missing high and medium risk patches and updates on OIG laptops listed by site and by type of laptop.

(U)

		Number of Laptops with Missing Patches or Updates[a]					
		3 or Fewer Patches					Total Missing More Than 3 Patches
Total	94	75 (80%)	12 (13%)	3 (3%)	0	4 (4%)	**19 (20%)**
Headquarters							
Atlanta Office							
Denton Office							
Primary							
Secondary							
Loaner							

[a] Includes the update missing from the model system as well as the two patches not applied to most of the laptops connected to the OIG Network.

(U) Source: OIG table based on the results of technical testing and interviews with OIG personnel.

(U) DHS policy requires that IT security patches be installed in accordance with configuration management plans or direction from DHS CSIRC. According to NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*, patching is critical to maintaining the operational availability, confidentiality, and integrity of information technology systems. NIST recommends that organizations have a systematic, accountable, and

documented process for managing exposure to vulnerabilities through the timely deployment of patches.

(U) Because the OIG had not applied all relevant patches and updates to its laptops, [redacted][15]

(U) An Accurate Inventory Is Needed For Property Management and Accountability

(U) The OIG has not established effective inventory management procedures for its laptop computers. We evaluated OIG procedures related to maintaining an accurate laptop inventory, returning equipment upon employee exit or transfer, handling lost or stolen laptops, clearing or sanitizing laptops before reuse or disposal, and the proper labeling of laptop computers.[16] Also, we reviewed laptop physical security measures, and assessed the OIG laptop inventory by analyzing the integrity of inventory data and conducting verification tests on the 31 laptop computers included in our manual review. The OIG has procedures to ensure that laptops are returned upon employee removal or transfer and for sanitizing laptops prior to disposal, as well as adequate laptop physical security measures. However, the OIG has not (1) maintained an accurate inventory; (2) cleared sensitive data from SBU laptops prior to reuse within the organization; (3) appropriately labeled its SBU laptops; or, (4) ensured that lost or stolen laptops were reported to the appropriate officials. As a result of the weaknesses in the OIG's inventory procedures, there is greater risk that laptop computers will not be configured

(U) [15] A denial of service attack is a form of attacking another computer to prevent legitimate users of a system from using the computer or its services.
(U) [16] Clearing requires overwriting all areas of the hard drive three times and then verifying the procedure by randomly re-reading the overwritten information. Sanitizing a hard drive requires incineration or degaussing (see evaluated degausser list at www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-9-12A.PDF).

and secured adequately, as evidenced by the weaknesses in the implementation of the OIG model system, and access to classified and sensitive information may not be restricted appropriately.

(U) Laptop Inventory is Not Accurate

(U) Although the OIG has an inventory of its classified and SBU laptops, it has not established procedures to ensure that inventory records are accurate. Specifically:

- (U) The OIG tracks purchased laptops, and conducts a serial number verification of laptops received. However, detailed information on laptop computers is not entered into the OIG inventory until after they are issued to users and a signed inventory sheet is returned to the ISSM or Information Systems Security Officer.
- (U) Although the OIG Helpdesk issues loaner and replacement laptops, the OIG has not issued procedures for this function. According to the ISSM, non-written procedures exist, but the OIG Helpdesk does not consistently follow those procedures.
- (U) The OIG has not established and communicated policies and procedures for conducting comprehensive periodic inventory reviews at OIG headquarters and field offices.

(U) In addition, there are a number of discrepancies in the OIG laptop inventory. For example, 50 of the 395 laptops listed in the OIG inventory did not have asset tag information entered, and 46 were missing serial numbers. Further, the laptop inventory does not include all OIG laptop computers. Specifically, two of the eight classified laptops and six of the 94 SBU laptops tested were not included in the inventory.

(U) According to the CIO, the OIG is researching options for addressing its IT inventory management issues, including the implementation of an enterprise property management system. However, no target implementation date for a new system has been established. Further, the CIO plans to conduct a complete computer inventory review during the 3rd quarter of fiscal year 2006. The review will include a complete laptop security controls review, as well as a

re-imaging of all laptops with a new model system, currently in development, based on the [redacted] operating system.

(U) DHS requires that components develop and maintain a property inventory of all portable electronic devices (PED), such as laptops. This inventory is to include serial numbers and/or seat numbers, user names, use, and location of all PEDs for accountability purposes.[17] Also, each DHS-owned PED is to have an asset tag, and included in the inventory. In addition, DHS requires that components conduct reviews, at least semiannually, of all equipment and software to ensure that only government-licensed software and equipment are being used, and that appropriate exceptions have been documented. As a result of these weaknesses in the OIG inventory, there is greater risk that laptop computers will not be configured and secured adequately.

(U) SBU Laptops Are Not Cleared Before Reuse

(U) The OIG has not implemented procedures to ensure that sensitive data is appropriately cleared or sanitized prior to the reuse or disposal of its SBU laptop computers. Specifically:

- (U) Laptops scheduled for reuse are not always cleared. According to the ISSM, laptops scheduled for reuse are usually re-imaged. In most cases, the OIG only clears a laptop when an employee specifically requests that it be done in order to protect sensitive data. According to the CIO and ISSM, the OIG has not implemented clearing procedures for all hard drives because they felt that the controls within Windows security profiles provided sufficient protections to ensure that the principle of least privilege is enforced. Nonetheless, the CIO plans to examine methods to implement the requirements of DHS' clearing policy.
- (U) Although the OIG has developed and disseminated *Excess Equipment Processing Procedures* to all field offices, during our review of the OIG Denton Field Office one of the responsible officials was preparing to release excess laptops with installed hard drives to a local

(U) [17] A seat, also referred to as a "node," is an intelligent element like a processor that can communicate using interprocessor communications. A seat is where entities and ports reside.

sheriff's office. The hard drives had been cleared using an employee's personal copy of a disk-wiping program. According to the CIO, this official had received copies of the OIG procedures and had complied with them in the past.

- (U) The OIG *Excess Equipment Processing Procedures* does not address the removal of labels or markings prior to the disposal of excess laptops. The ISSM stated that the removal of labels and markings is usually communicated in e-mail notifications of disposal procedures. The OIG is planning to include written procedures addressing this step in an upcoming release of the *Excess Equipment Processing Procedures* document, but a date for the revision has not been established.

(U) DHS policy requires that components ensure that any information system's storage medium containing sensitive information be cleared using approved clearing methods before it is reused within the organization. DHS policy also requires that components ensure that any information system's storage medium containing sensitive information be sanitized using approved sanitization methods before it is disposed of, recycled, returned to the owner, or returned to the manufacturer. Sanitization also includes the removal of all labels, markings, and activity logs. As a result of these weaknesses in the OIG process for clearing and sanitizing laptop computers, there is greater risk that access to sensitive information may not be limited adequately.

(U) Laptops Are Not Appropriately Marked

(U) The OIG has not ensured that its laptops are appropriately labeled. Specifically,

- (U) None of the SBU laptops included in our review were labeled indicating that the units were not authorized for classified processing. According to the CIO, the OIG had not affixed labels to the SBU laptops because the requirement was not included in the labeling guidelines in the DHS Handbook, and instead was included as part of the DHS warning banner policy and thus overlooked.
- (U) One of the classified laptops did not have classification stickers affixed indicating the highest level of classification of information that

has ever been processed or stored on the device. According to the ISSM, the laptop did not have classification stickers because it was not purchased and configured by the CIO's staff.

(U) DHS policy requires that all laptop computers not authorized to process classified information have a label affixed indicating, "This machine is not authorized for classified processing." DHS policy also requires that all equipment be marked with the highest level of classification of information that has ever been processed or stored on the device. Because these laptops were not appropriately marked, there is greater risk that classified information may have been processed on an unclassified system.

(U) Lost or Stolen Laptops Are Not Appropriately Reported

(U) The OIG has not ensured that lost or stolen laptops are reported to the DHS CSIRC. The OIG has established standard operating procedures for use by the Helpdesk to address lost or stolen laptops. In the event a laptop is lost or stolen, the Helpdesk is required to notify the OIG Office of Security and the ISSM. The ISSM is then responsible for notifying the DHS CSIRC. However, a security incident involving a stolen OIG laptop in 2005 was not reported to the DHS CSIRC. According to the ISSM, the incident was reported directly to the OIG Office of Security, but was not reported to the ISSM until several months later, and thus was not reported to the DHS CSIRC.

(U) DHS policy requires that components report significant computer security incidents to the DHS CSIRC immediately upon identification and validation of incident occurrence. The DHS CSIRC is normally responsible for initiating any disciplinary action following investigation of a security event by notifying appropriate law enforcement authorities, who pursue the investigation and recommend disciplinary action, if required. Because the OIG had not reported the security incident to the DHS CSIRC, senior DHS officials may not be aware of the extent or scope of laptop security issues at the department, and the appropriate corrective actions may not have been taken. Further, without an accurate and current inventory, the OIG may be unaware of additional laptops that are missing.

(U) FISMA Requirements

(U) The OIG has not fulfilled facets of its security program required by FISMA.[18] We evaluated the effectiveness of the OIG's information security program and practices as implemented for SBU laptop computers to determine whether DHS continues to make progress in implementing its agency-wide information security program. The OIG has implemented many of the security program requirements for the OIG Network. However, significant work remains for the OIG to implement necessary security program requirements. See Appendix C for the results of our FISMA evaluation.

(U) RECOMMENDATIONS

(U) To protect OIG government-issued SBU laptop computers, we recommend that the Assistant Inspector General for Administrative Services instruct the CIO to:

1. (U) Remedy the existing critical vulnerabilities in the standard configuration for SBU laptops, based on DHS and federal configuration guidelines, and determine whether similar vulnerabilities and remediation are relevant to all government-issued computers.
2. (U) Establish procedures to ensure that model systems are configured to protect OIG data and verified prior to implementation.
3. (U) Develop procedures to ensure that all OIG laptops are patched and updated in a timely manner, including loaner and secondary unit laptops, as well as all government-issued computers.
4. (U) Implement an enterprise property management system to ensure that an accurate laptop inventory is maintained, and ensure that all laptop computers are handled in accordance with OIG inventory management policies and procedures.
5. (U) Clear or sanitize laptop computers before reissue or disposal, and ensure that classified and SBU laptops are labeled appropriately, in accordance with DHS and federal guidelines.

(U) [18] FISMA is included under Title III of the E-Government Act of 2002 (Public Law 107-347).

6. (U) Implement FISMA security program requirements for the OIG Network. Specifically, the CIO should develop a risk assessment, test the contingency plan, and provide specialized privacy training to appropriate officials.

(U) MANAGEMENT COMMENTS AND OIG ANALYSIS

(U) The OIG concurs with recommendation 1. The OIG has created a new master image for SBU laptop computers with additional security controls that address the vulnerabilities identified during the review. The OIG CIO will document vulnerabilities not addressed in the OIG's master image as acceptable risks.

(U) We accept the OIG's response to create a new master image for its SBU laptop computers. The Designated Accrediting Authority should formally approve vulnerabilities that the OIG CIO plans to document as an acceptable risk. In addition, we maintain that the OIG should determine whether similar vulnerabilities and remediation are relevant to all OIG government-issued computers.

(U) The OIG concurs with recommendation 2. The OIG has revised and tested its implementation procedures on a series of recently purchased laptops. The procedures are aligned with DHS and other federal standards. Also, the OIG has modified its change management program to ensure that changes to the standard configuration are tested for vulnerabilities before being applied to its computers.

(U) We accept the OIG's response to enhance its procedures to ensure that model systems are configured to protect OIG data and verified prior to implementation.

(U) The OIG concurs with recommendation 3. The OIG is addressing areas in the patch management procedures that require strengthening. OIG technicians have successfully applied all missing patches. Laptop computers that were identified as having major patch problems have been individually addressed and corrected or removed from circulation. In addition, the OIG CIO is

updating its existing patch management procedures to include a review and validation process to ensure that all patches are properly and successfully applied on all OIG issued equipment. All loaner and secondary units that are not regularly connected to the OIG network will be placed on a schedule requiring routine connection to the network to allow the automated patch procedure to be performed.

(U) We accept the OIG's response to enhance its procedures to ensure that all OIG laptops are patched and updated, including loaner and secondary unit laptops, as well as all OIG government-issued computers.

(U) The OIG concurs with recommendation 4. The OIG CIO is currently participating in a review of the Department's Sunflower Property Management System to ensure that information technology assets are sufficiently addressed and can be adequately captured in the future enterprise system. While a decision is pending on the final enterprise solution, the existing OIG inventory will be verified and updated to facilitate transfer of this data into the future enterprise system. The target date for the OIG to complete its physical inventory is September 2006.

(U) We accept the OIG's plan of action to convert its information technology assets to a new property management system and to update its current inventory to facilitate the transfer of data. To comply with DHS inventory management policies and procedures, the OIG's physical inventory should also include a review of authorized and installed software.

(U) The OIG concurs with recommendation 5. The OIG's current excess property procedures require that all hard drives be removed and returned to the IT Division for proper destruction. In addition, hard drives are removed from computers prior to any service calls where the computers are returned to the vendor or service provider. The OIG CIO is modifying existing procedures to require the removal of hard drives from systems slated for re-issue within the OIG environment. The hard drives will be properly cleared and sanitized before they are distributed for re-use. In addition, the OIG plans to appropriately label its laptop computers, according to classification, by September 2006.

(U) We accept the OIG's response to enhance its procedures to ensure that all hard drives are removed for destruction or cleared and sanitized for re-use in the OIG environment; and that classified and SBU laptops are labeled appropriately in accordance with DHS and federal guidelines.

(U) The OIG concurs with recommendation 6. In October 2005, the OIG submitted a remediation plan to the DHS Information Security Officer for all outstanding FISMA related documentation. The OIG will have all appropriate FISMA documentation completed by September 2006. In addition, the OIG is establishing a privacy-training program and developing a training plan for all employees and contractors, to be completed by September 2006.

(U) We accept the OIG's response to develop a risk assessment, test its contingency plan, and establish a privacy-training program for all employees and contractors.

(U) Purpose, Scope, and Methodology

(U) The objective of this audit was to determine whether the OIG had implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptop computers. Specifically, we determined whether the OIG had implemented adequate (1) policies and procedures for inventory management; (2) physical security measures; (3) logical access controls; and, (4) wireless security measures for sensitive data contained in its government-issued laptops. Our focus was to test the development and implementation of an adequate model system for the laptop computers processing and storing sensitive or classified DHS data, as well as the procedures used to patch and update laptops once placed into operation. In addition, we obtained FISMA information required for the OIG's annual independent evaluation.

(U) To identify sensitive and classified laptop computers, we analyzed the OIG laptop computer inventory as of November 2005. Based on our review of the laptop inventory, we selected the following OIG sites for testing:

(U) OIG Testing Locations and Laptop Computers

	User Assigned			
OIG Headquarters Washington, DC				
OIG Field Office Atlanta, GA				
OIG Field Office Denton, TX				

(U) In addition, we performed extensive manual security parameter checks on select laptop computers to confirm the results of our scans and identify any additional security weaknesses. Upon completion of the tests, we provided component officials with technical reports detailing the specific vulnerabilities detected on their system and the actions needed for remediation.

Appendix A
Purpose, Scope, and Methodology

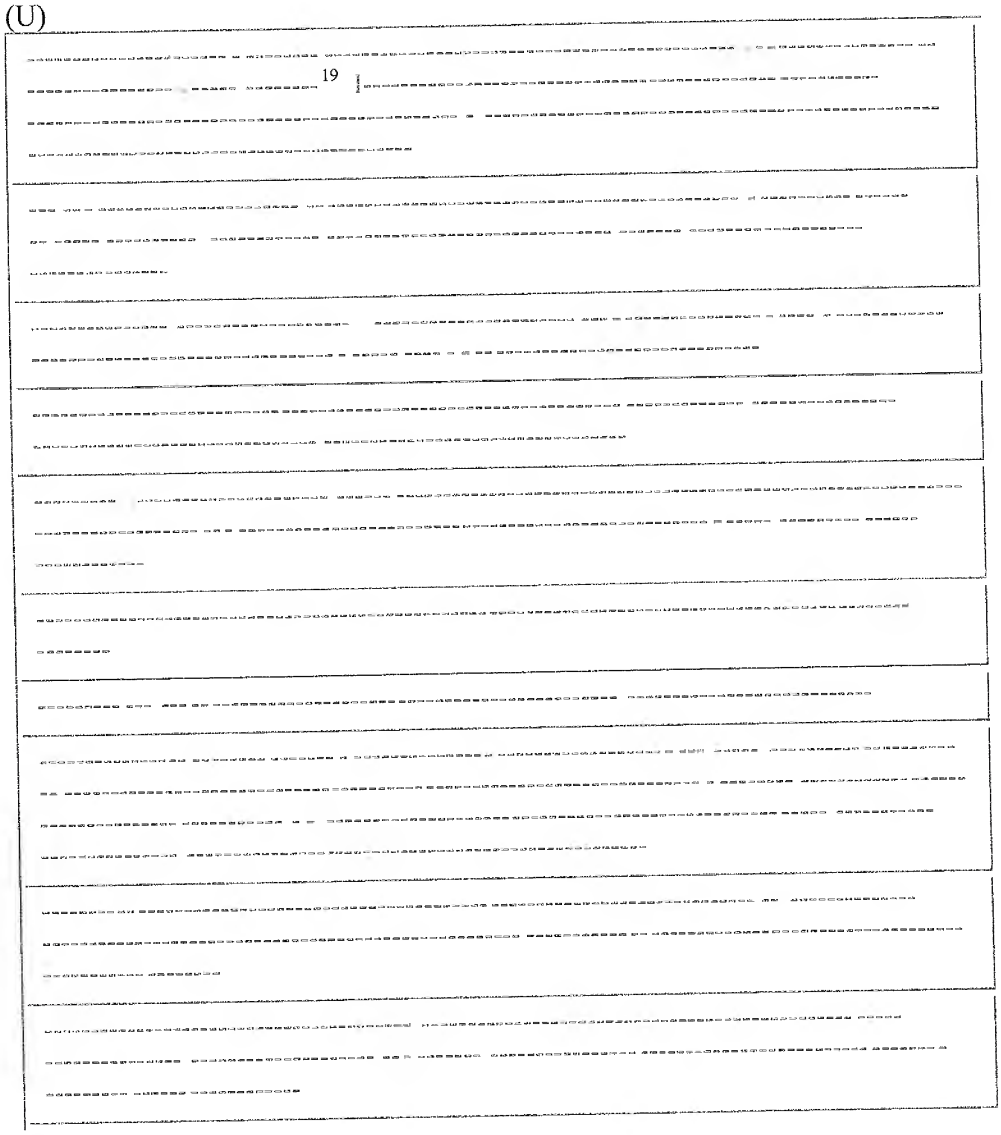
(U) We conducted fieldwork at the OIG headquarters in Washington, DC; OIG field offices in Atlanta, GA, and Denton, TX; and, the OIG's ATL. We conducted our audit from December 2005 through January 2006 under the authority of the Inspector General Act of 1978, as amended. Because we reviewed the OIG CIO office and included laptop computers assigned to the OIG Office of IT Audits, the appearance of a conflict of interest may exist. However, during our audit we reviewed laptops assigned to all OIG offices, and we included all review findings in our report. We conducted all audit work according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix E.

(U) Our principal points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits at (202) 254-4100 and Edward G. Coleman, Director, Information Security Audit Division at (202) 254-5444.

Appendix A
Purpose, Scope, and Methodology

(U) We used 10 testing tools to conduct internal security tests to evaluate the effectiveness of controls implemented for the systems:

(U)



(U) [19]

(U)

(U) *Source: OIG auditors conducting security scans on laptop computers in Austin, TX.*

(U)

(U) *Source: OIG auditors conducting security scans on laptop computers at OIG Headquarters in Washington, DC.*

Appendix B
Management's Response

(S)

June 14, 2006

Homeland Security

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology Audit

FROM: Edward Cincinnati
Assistant Inspector General for Administration

SUBJECT: Management Response to the Draft Report titled:
OIG Laptop Computers are Susceptible to Compromise (S)

(U) Thank you for the opportunity to provide comments on the subject report. The observations and recommendations contained in the report are consistent with our plans for improving the Office of Inspector General (OIG) Information Security Program, specifically as it relates to the security and protection of information processed on OIG laptops. The OIG CIO has reviewed and concurs with the recommendations, and has generated a plan of action and milestones addressing the findings contained in the report.

(U) Our specific response to each of the recommendations contained in the report is provided below.

(U) Sensitive But Unclassified (SBU) Recommendations

(U) Recommendation # 1: Remedy the existing critical vulnerabilities on the standard configuration for SBU laptops, based on DHS and federal configuration guidelines, and determine whether similar vulnerabilities and remediation are relevant to all government-issued computers.

(U) DHS-OIG Response: Prior to the draft report issue date, a new master image for OIG SBU laptop computers was created with additional security controls implemented, addressing vulnerabilities identified during the review. The new image was presented to the IT auditors and re-scanned, at which time the auditors validated that the identified vulnerabilities were addressed.

In summary, the new image incorporated required configuration changes related to 6 specific settings that addressed 321 high risk vulnerabilities, and 13 settings that addressed 1,284 medium risk vulnerabilities.

(U) Recommendation # 2: Establish procedures to ensure that model systems are configured to protect OIG data and verified prior to implementation.

(U) DHS-OIG Response: Prior to the draft report issue date, the OIG CIO addressed the problems identified in the report related to the need to establish procedures for consistent application of the standard OIG master image on all laptop equipment. The revised procedures were implemented and tested on a series of recently purchased laptops. The new

(S)

procedures include configuring the master image based on DHS and other federal standards, scanning the image for vulnerabilities, validating the security hardening established on the laptop, and documenting the configuration parameters.

(U) In addition, the OIG has modified its change management program to ensure that as laptops are released to the user community after initial burn-in and the standard configuration has been applied, subsequent changes to the configuration (i.e., loading additional software on the unit) are tested for vulnerabilities before the unit is released back to the end-user. The new process was exercised during the review.

Once the OIG CIO was notified by the auditors of the vulnerabilities associated with these units, they were immediately pulled from circulation and re-configured to the OIG standard image, removing the
Additionally, the older Toshiba notebooks identified in the report are in the process of being recalled and re-imaged from a new hardened master image, following the OIG's established configuration procedures.

(U) Recommendation # 3: Develop procedures to ensure that all OIG laptops are patched and updated in a timely manner, including loaner and secondary unit laptops, as well as all government-issued computers.

(U) DHS-OIG Response: The OIG CIO has reviewed existing patch management procedures, and addressed areas in the procedures that require strengthening. The existing process applies current patches to all workstations or laptops at the time the units connect to the OIG network.

OIG technicians were able to resolve the problem and reapply those patches. In addition, all computers identified in the report as having major patch problems have been either removed from circulation or individually addressed and corrected. Those units removed from circulation will not be re-distributed until they have been successfully configured to OIG standards.

(U) In addition to the corrective action previously discussed, the OIG CIO has directed OIG technicians to update existing patch management procedures to include a review and validation step, to ensure that all patches are properly and successfully applied on all OIG issued equipment. The inventory of loaner and secondary units that are not regularly connected to the OIG network will be placed on a schedule requiring routine connection to the network to allow the automated patch procedure to be performed on these laptops.

(U) Recommendation # 4: Implement an enterprise property management system to ensure that an accurate laptop inventory is maintained, and ensure all laptop computers are handled in accordance with OIG inventory management policies and procedures.

(U) DHS-OIG Response: The OIG understands the importance of implementing a sound process to account for all OIG issued laptops. The OIG CIO is currently participating in a review of the Department's Sunflower Property Management System, as part of a project

(S)

initiated by the Assistant Inspector General for Administration. The OIG CIO is participating in the review to ensure information technology assets are sufficiently addressed and can be adequately captured in the future enterprise system. While a decision is pending on the final enterprise solution, the OIG CIO has initiated a project to conduct an OIG-wide, physical inventory of all OIG laptops. Data in the OIG's existing inventory database will be verified and/or updated as required during the inventory process, to facilitate transfer of this data into the future enterprise system. The target completion date for the physical inventory is September 2006.

(U) Recommendation # 5: Clear or sanitize laptop computers before reissue or disposal, and ensure that classified and SBU laptops are labeled appropriately, in accordance with DHS and federal guidelines.

(U) DHS-OIG Response: As part of the OIG's existing excess property procedures, all hard drives are required to be removed and returned to the IT Division for transportation to NSA for proper destruction. In addition, all hard drives are removed prior to any service calls requiring the return of the computer equipment to the vendor or service provider. All non-operational hard drives are returned to the IT Division for destruction. The OIG CIO is in the process of modifying the existing procedures to require the removal of hard drives from systems slated for re-issue within the OIG environment. These hard drives will be sent back to the IT Division to be properly cleared and sanitized before they are distributed for re-use. The IT Division will maintain a pool of replacement hard drives that have been sanitized, with the standard OIG image applied, to facilitate and expedite the replacement process. Additionally, the OIG Information Systems Security Manager is in the process of obtaining the external labels required to properly mark laptops according to their classification. All OIG laptops will be appropriately labeled before the end of FY 06.

(U) Recommendation # 6: Implement FISMA security program requirements for the OIG Network. Specifically, the CIO should develop a risk assessment, test the contingency plan, and provide specialized privacy training to appropriate officials.

(U) DHS-OIG Response: On October 12, 2005, the OIG submitted the OIG's system remediation plan, which addressed all outstanding FISMA related documentation, to the DHS Information Security Officer. The plan was submitted prior to the DHS established deadline of August 2006, and addressed the requirements for developing a network risk assessment, and tests of the contingency plan. The OIG Information System Security Manager will have the appropriate documentation related to these areas completed by the end of FY 06. The OIG CIO is also working with the Assistant Inspector General for Administration and the Office of Counsel to establish a privacy-training program for OIG employees and contractors, and develop a training plan by the end of FY 06.

(S)

(S)

(S)

DHS OIG Response to Laptop Report
Page 4 of 4

(S)

(S)

(S)

(U) Recommendation # 3: Implement the FISMA security program requirements for the OIG Secure Classified System, including certifying and accrediting the system, testing and evaluating security controls, establishing and testing a contingency plan, as well as providing specialized privacy training to relevant officials.

(U) DHS-OIG Response: The classified system is currently undergoing C&A, and the related artifacts are under review. The OIG's system remediation plan, submitted to the DHS Information Security Officer in October 2005, addresses all outstanding FISMA related documentation. The OIG CIO plans to have the classified systems fully certified and accredited by September 2006.

(U) The OIG CIO has directed OIG technicians to establish a process for scheduling routine test and evaluation of the security controls implemented for these units. The OIG CIO is also working with the Assistant Inspector General for Administration and the Office of Counsel to establish a specialized privacy-training program for appropriate officials.

(U) FISMA Requirements

(U) Title III of the *E-Government Act*, entitled FISMA, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets.[20] The agency's security program should provide security for the information as well as the systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

(U) To comply with OMB's FISMA reporting requirements, we evaluated the effectiveness of the OIG's information security program and practices as implemented for SBU laptop computers to determine whether DHS continues to make progress in implementing its agency-wide information security program. We collected information relative to certification and accreditation (C&A), system impact level determination, NIST SP 800-26 annual assessment, assessment of E-authentication risks, specialized security training, and POA&Ms.[21]

(U) Our evaluation of the OIG laptop system shows that the component has not implemented certain security management practices into its information security program, as required by FISMA.

(U) [20] The E-Government Act of 2002 (Public Law 107-347), signed into law on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.
(U) [21] As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, and NIST 800-63, *Electronic Authentication Guideline.*

(U) Table 4: FISMA Compliance Metrics

FISMA Reporting Requirements	
Does the system have a complete and current C&A?	The OIG Network system was granted authority to operate on June 24, 2005.
Has the system's impact level been determined according to FIPS-199 criteria?	
Does the system have a complete and current NIST SP 800-26 annual assessment?	The OIG Network has a security plan, but the risk assessment is currently in draft. The OIG plans to complete the risk assessment by the end of February 2006.
Were the system's security controls tested and evaluated in the last year?	
Has a system contingency plan been established and tested?	The OIG Network has a contingency plan dated November 2005, but the plan has not been tested.
Has an assessment of E-Authentication risk been performed for the system?	
Have personnel with significant security responsibilities obtained specialized security training?	
Have individuals involved in the administration of IT systems, or with significant security responsibilities, obtained specialized privacy training?	
Are POA&Ms created and managed for the system?	POA&Ms have been created and entered into the DHS FISMA reporting system.

(U) *Source: OIG table based on interviews with OIG personnel and analysis of database documentation.*

(S) [redacted] Will Enhance Laptop Security

(S) [redacted]

(U) We evaluated the process used by the OIG to [redacted] Also, we evaluated the procedures used to patch and update classified laptops. In addition, to comply with the Office of Management and Budget's (OMB) *Federal Information Security Management Act of 2002* (FISMA) reporting requirements, we evaluated the effectiveness of the OIG's information security program as implemented for the OIG Secure Classified System.[22]

(S) [redacted]

- (S) [redacted][23]

(U) [22] FISMA is included under Title III of the E-Government Act of 2002 (Public Law 107-347).
(S) [23] [redacted]

- (S)
- (S)
- (S)
- (S)
- (S)
- (S)

(S)

(S) [24]

(U) Further, the OIG has not fulfilled facets of its security program required by FISMA. Specifically, (1) the classified laptop system has not been certified and accredited, (2) security controls for the classified system have not been tested and evaluated within the last year, (3) specialized privacy training has not been provided to individuals involved in the administration of personal information systems or with significant information security responsibilities; and, (4) the classified system does not have an approved contingency plan. As a result, classified and sensitive information stored or processed on the OIG's laptop computers may not be protected adequately.

(U) Table 5: FISMA Compliance Metrics

FISMA Reporting Requirements	Classified System	Notes
Does the system have a complete and current certification and accreditation (C&A)?	**No**	The C&A for the classified system is scheduled for completion in March 2006.
Has the system's impact level been determined according to FIPS-199 criteria?	Yes	The system impact level was determined to be High for confidentiality, integrity, and availability.
Does the system have a complete and current NIST SP 800-26 annual assessment?	Yes	A self-assessment for the classified system was completed in August 2005.
Does the system have a security plan and risk assessment?	Yes	The documents were created as part of the C&A process.
Were the system's security controls tested and evaluated in the last year?	**No**	The classified system is currently undergoing C&A, and a security test and evaluation (ST&E) will be performed as part of the C&A process.
Has a system contingency plan been established and tested?	**No**	The classified system is currently undergoing C&A, and a contingency plan will be developed as part of the C&A process.
Has an assessment of E-Authentication risk been performed for the system?	N/A	Remote users do not authenticate to the classified systems for the purposes of conducting government business electronically.
Have personnel with significant security responsibilities obtained specialized security training?	Yes	As of January 25, 2006, 6 of the 8 personnel with significant security responsibilities had received specialized security training.
Have individuals involved in the administration of IT systems, or with significant security responsibilities, obtained specialized privacy training?	**No**	As of January 31, 2006, specialized privacy training had not been scheduled.
Are plans of action and milestones (POA&M) created and managed for the system?	Yes	Most POA&Ms for the classified laptops are maintained outside the FISMA reporting system due to their sensitivity.

(U) Source: OIG table based on interviews with OIG personnel and analysis of database documentation.

(S) [redacted]

(S) [redacted]

(S) [redacted]

(S) [redacted]

(U) Recommendations

(U) To protect OIG government-issued classified laptop computers, we recommend that the Assistant Inspector General for Administrative Services instruct the Chief Information Officer to:

1. (S)
2. (S)
3. (U) Implement FISMA security program requirements for the OIG Secure Classified System, including certifying and accrediting the system, testing and evaluating security controls, establishing and testing a contingency plan, as well as providing specialized privacy training to relevant officials.

(U) Management Comments and OIG Analysis

(S)

(S)

[redacted]

(S) [redacted]

(S) [redacted]

(U) The OIG concurs with recommendation 3. The OIG classified system is currently undergoing C&A and its related artifacts are under review. The OIG's system remediation plan was submitted to the DHS Information Security Officer in October 2005. The OIG CIO plans to have the classified system fully accredited by September 2006. In addition, the OIG CIO is establishing a process to routinely test and evaluate security controls for classified laptop computers and to provide specialized privacy training to appropriate officials.

(U) We accept OIG's response to implement corrective action plans to C&A its classified system; and, to establish a process to test security controls and provide specialized privacy training to relevant officials.

Appendix E
Major Contributors to this Report

(U) Information Security Audits Division
Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Jason Bakelar, Audit Team Leader
William Matthews, Auditor
Eugene Yu, Auditor
Domingo Alvarez, Referencer

(U) Advanced Technology Division
Chris Hablas, Senior Security Engineer

(U) Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Policy
DHS GAO/OIG Audit Liaison
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative and Intergovernmental Affairs
Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison

(U) Office of Inspector General

Inspector General
Deputy Inspector General
Chief Information Officer

(U) Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

(U) Congress

Congressional Oversight and Appropriations Committees, as appropriate

~~SECRET~~

(U) Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

(U) OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.